



The
CrossCheck
Portal



—Organic light-emitting diodes (OLEDs) are promis- ing new large-area light sources on their way to commercialization. However, there is still much room for improvement in terms of device efficiency and long-term stability under ambient conditions.

In this article, we review the current status of efficiency analysis based on optical simulations of state-of-the-art OLED stacks. In detail, we present a method to determine the effect of emitter efficiency of the emitter, figure out the critical points for non-isotropic emitter orientation and discuss the application of the developed method to analyze degradation effects during electrical operation under various terms—device efficiency, optical properties, non-isotropic emitter orientation, degradation, organic light-emitting diodes, and introduction of new materials.

electroluminescent devices", *Physical Review B*, 03/2012 [?] 72 words / 1% - Internet from Wed Nov 28, 2012 [as.wiley.com](#) [?]

66 words / 1% - CrossCheck [?] Shih-Hsueh, "Mechanism of enhanced light emission from an emitting layer embedded in metal-insulator-metal structures", *Physical Review B*, 07/2010 [?]

59 words / 1% - CrossCheck [?] "Efficiency analysis of organic light-emitting diodes", *Optics Express*, 07/2010 [?]

54 words / 1% - Internet from Fri Dec 03, 2010 [ledetd.mis.nsysu.edu.tw](#) [?]

52 words / 1% - Internet from Tue Jun 07, 2011 [pcphotonics.intec.ugent.be](#) [?]

48 words / 1% - CrossCheck [?] Krummacher, B.C., "Efficiency analysis of organic light-emitting diodes based on optical simulation", *Organic Electronics*, 200905 [?]

48 words / 1% - CrossCheck [?] "Efficiency analysis of organic light-emitting diodes based on optical simulation", *Organic Electronics*, 200905 [?]

39 words / < 1% match - CrossCheck [?] G. Li, "Electroluminescence-detected magnetic resonance studies of Pt octaethyl porphyrin-based phosphorescent organic light-emitting devices", *Physical Review B*, 06/2005 [?]

User's Guide for the IEEE CrossCheck Portal and Prohibited Authors List Database

Part 1

Overview of the IEEE CrossCheck Portal

Part 2

Reviewing and Interpreting Similarity Reports

Part 3

Overview of the Prohibited Authors List Database

Part 1. Overview of the IEEE CrossCheck Portal

Introduction

The IEEE Intellectual Property Rights Office is pleased to offer two important quality-control tools to publication volunteers. The CrossCheck Portal and the Prohibited Authors List Database are both available on one site, and can be accessed easily.

What Is CrossCheck?

CrossCheck is a plagiarism detection tool that conducts high-speed comparisons of submitted manuscripts against a very large database of published technical papers (as well as over 6 billion web pages), with the result that reports will rate all submissions for similarities to previously published works. The publisher can then follow up to isolate and review the high-scoring papers as necessary.

Plagiarism detection systems are only as effective as the amount and quality of the source content within them. CrossCheck's significant advantage over all other similar services is that it includes the indexed, full-text content of participating CrossCheck member publishers.

What Is the IEEE CrossCheck Portal?

The IEEE CrossCheck Portal is a web tool and service that brings the functionality of the CrossCheck tool together with an IEEE interface made available to IEEE publications volunteers at no charge. Checking your conference papers with the portal will help to insure that only the best, plagiarism-free papers get published. In addition, you will receive IEEE IPR Office staff support to help you check the integrity of the submitted manuscripts.

Who Should Use the IEEE CrossCheck Portal?

The IEEE CrossCheck Portal is available to **all** IEEE publication volunteers including IEEE journal editors and IEEE conference organizers. Publications that will not be transferring copyright to IEEE may not use the portal.

Where to Find the Portal and How to Sign Up

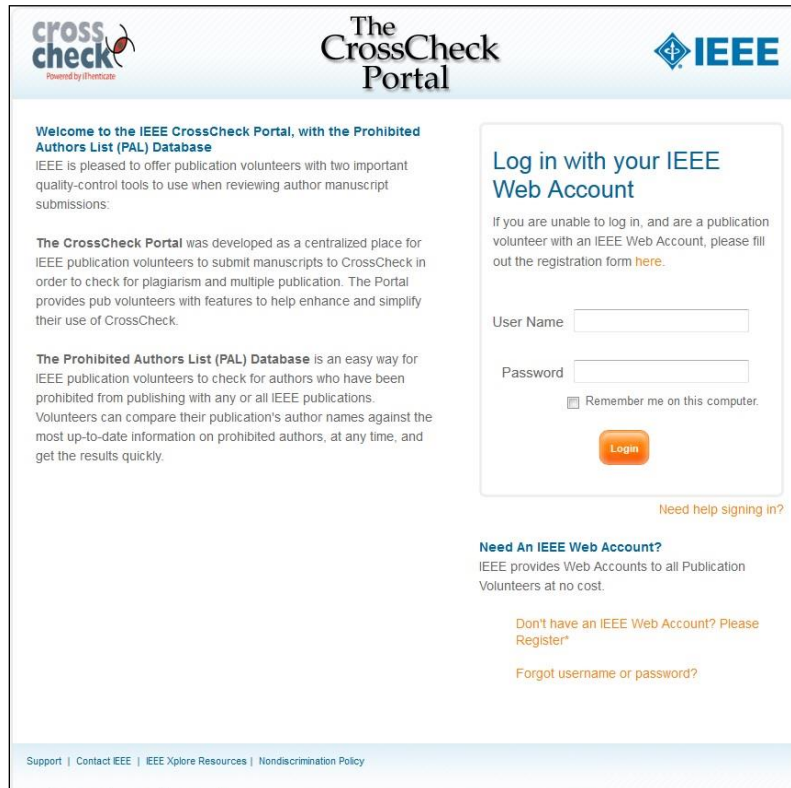
Volunteers who are interested in using the Portal can contact the IEEE IPR Office through a registration form located on the following web site:

http://www.ieee.org/publications_standards/publications/rights/crosscheckportal.html

Logging into the CrossCheck Portal

You will need to use your IEEE Web Account credentials to log into the Portal. IEEE Web Accounts are available to IEEE members and IEEE Society members. If you are not an IEEE member and do not have an IEEE Web Account, please contact the IEEE IPR Office at crosscheckportal@ieee.org for more information.

- Enter your user name and password
- Click the **Login** button



The screenshot shows the IEEE CrossCheck Portal login interface. At the top, there are logos for 'crosscheck' (Powered by iParade), 'The CrossCheck Portal', and the IEEE logo. The main content area is divided into two columns. The left column contains a welcome message and two sections: 'The CrossCheck Portal' and 'The Prohibited Authors List (PAL) Database'. The right column features a login box with the heading 'Log in with your IEEE Web Account', a brief instruction, and input fields for 'User Name' and 'Password'. Below the password field is a 'Remember me on this computer' checkbox and an orange 'Login' button. Below the login box are links for 'Need help signing in?', 'Need An IEEE Web Account?', 'Don't have an IEEE Web Account? Please Register*', and 'Forgot username or password?'. At the bottom, a footer bar contains links for 'Support', 'Contact IEEE', 'IEEE Xplore Resources', and 'Nondiscrimination Policy'.

Welcome to the IEEE CrossCheck Portal, with the Prohibited Authors List (PAL) Database
IEEE is pleased to offer publication volunteers with two important quality-control tools to use when reviewing author manuscript submissions:

The CrossCheck Portal was developed as a centralized place for IEEE publication volunteers to submit manuscripts to CrossCheck in order to check for plagiarism and multiple publication. The Portal provides pub volunteers with features to help enhance and simplify their use of CrossCheck.

The Prohibited Authors List (PAL) Database is an easy way for IEEE publication volunteers to check for authors who have been prohibited from publishing with any or all IEEE publications. Volunteers can compare their publication's author names against the most up-to-date information on prohibited authors, at any time, and get the results quickly.

Log in with your IEEE Web Account
If you are unable to log in, and are a publication volunteer with an IEEE Web Account, please fill out the registration form [here](#).

User Name:

Password:

☐ Remember me on this computer.

[Login](#)

[Need help signing in?](#)

Need An IEEE Web Account?
IEEE provides Web Accounts to all Publication Volunteers at no cost.

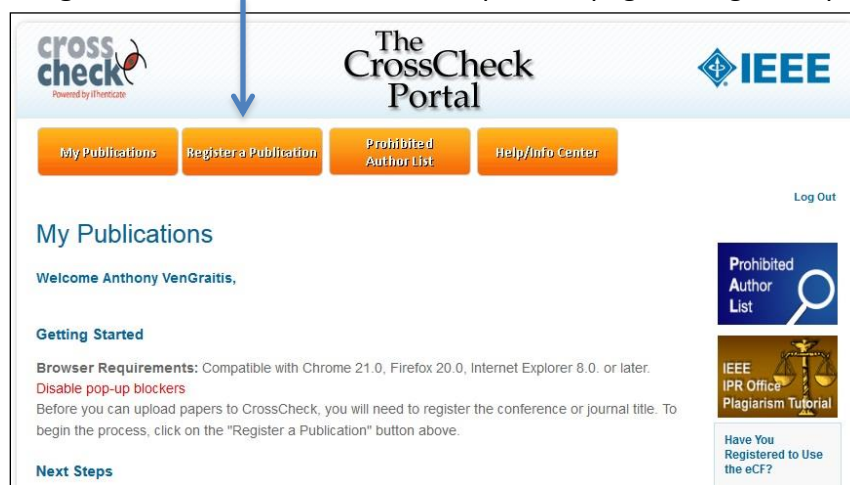
[Don't have an IEEE Web Account? Please Register*](#)

[Forgot username or password?](#)

[Support](#) | [Contact IEEE](#) | [IEEE Xplore Resources](#) | [Nondiscrimination Policy](#)

Once you are logged in, you will arrive on the “My Publications” page. This page will act as your own dedicated and secure page to access publications that you have registered in the Portal. As a new user, this page will not list any information. You will need to register your publication titles to begin using CrossCheck.

- Click the **Register a Publication** tab at the top of the page to begin the process.



Registering a New Publication

On the “Registering a New Publication” page, you will need to complete all the fields to add a new publication title to your list. Please fill out the following information:

- Name
- Email
- Publication or Conference Title
- Conference Number (if available)—This will be the 5-digit conference ID assigned to your conference by IEEE
- Publication Date
- Conference Sponsorship Level (fully or cosponsored)

Click the **Continue** button to complete the registration.

The publication title will now appear on the “My Publications” page

My Publications Page

Your newly registered publication will appear on the page with the following items

- Publication Title
- Papers Uploaded
- Alerts
- Delete

There will also be a link “Upload” at the far right of the table. Clicking this link will bring you to the “Manuscript Upload” page.

crosscheck
Powered by iThenticate

The CrossCheck Portal

IEEE

My Publications Register a Publication Prohibited Author List Help/Info Center

Log Out

Admin Tool

My Publications

Welcome Anthony VenGraitis,

Getting Started

Browser Requirements: Compatible with Chrome 21.0, Firefox 20.0, Internet Explorer 8.0. or later.
Disable pop-up blockers
 Before you can upload papers to CrossCheck, you will need to register the conference or journal title. To begin the process, click on the "Register a Publication" button above.

Next Steps

To upload papers to CrossCheck, click on the "Upload" link to the right of the publication title.
 To review CrossCheck results, click on the publication title.
 To add another publication title, click on the "Register a Publication" button above.

Publication Title	Papers Uploaded	Alerts	Delete
Conference Proceedings Title	0	0	Upload

Prohibited Author List

IEEE IPR Office Plagiarism Tutorial

Have You Registered to Use the eCF?

The electronic IEEE Copyright Form (eCF) is a highly effective tool that transfers ownership rights of the intellectual property to IEEE, and also saves significant amounts of time and effort on the part of IEEE authors, volunteers and staff.

Uploading Your Content to CrossCheck

Now that you have your publication registered in the Portal, you can begin uploading papers to CrossCheck. CrossCheck can only accept the following file types for uploading:

- Portable Document Format (PDF)
- Microsoft Word (DOC and DOCX)
- Plain Text (TXT)
- HTML
- Rich Text Format (RTF)

To upload only one manuscript, click on the **“Single File Upload”** link. A search window will appear that will let you browse your computer and select the file.

The screenshot shows the 'The CrossCheck Portal' interface. At the top, there are logos for 'cross check' (Powered by iThenticate), 'The CrossCheck Portal', and 'IEEE'. Below these are navigation buttons: 'My Publications', 'Register a Publication', 'Prohibited Author List', and 'Help/Info Center'. On the right, there are links for 'Log Out' and 'Admin Tool'. The main heading is 'Manuscript Upload Page'. Below this, it states: 'CrossCheck accepts the following file types for upload: Portable Document Format (PDF), Microsoft Word (DOC and DOCX), Plain Text (TXT), HTML, Rich Text Format (RTF)'. It then explains the upload methods: 'Select the method of upload. You may submit individual files or a zip file. If you have many files to submit, you should use the "Zip File Upload" method to submit multiple files for batch uploads.' Two options are listed: 'Single File Upload (PDF, DOC, ETC)' with a processing time of '5-10 minutes per file', and 'Zip File Upload' with a processing time of 'Up to 4-8 hours'. A dotted arrow points from the 'Single File Upload' link to a file selection dialog box that is overlaid on the page. The dialog box has a title bar, a 'Select a file to upload' prompt, a 'Browse...' button, and a 'No file selected.' message. Below this, it says 'Note: Individual manuscript file size must not exceed 15MB. Total zip file size must not exceed 200MB.' and has 'Submit' and 'Cancel' buttons. On the right side of the portal, there is a 'Prohibited Author List' button and a sidebar with links for 'Author List', 'IEEE IPR Office Plagiarism', and 'Have You Registered the eCF?'. At the bottom right, there is a small text block about the electronic Copyright Form.

The Portal also can accept zip files for batch uploads of manuscripts. The zipped file size can be up to 200 MB total and contain up to 1000 individual manuscript files (each manuscript file must be less than 15 MB). Click on the “**Zip File Upload**” link and select the zip file on our computer.

Single file uploads will be processed at once, and should be completed within 5-10 minutes. Zip files will require more time, and so after you have uploaded your manuscripts, you will be sent an email notification once the processing has been completed.

Please Note: Depending on the size of your zip file and traffic from other Portal users, the process could take as much as 8 hours. Please plan accordingly when using the Portal.

Email Notification that Uploaded Files have been Processed

After your zip files have been processed and reports are ready, you will be sent an email with details on accessing the reports (along with the IPR Office staff, who will help to review the results). If there were any problems processing your files, you will be given more information

about the types of problems and instructions on how to resolve them. You will then need to correct and resubmit files that were not processed the first time. If you uploaded a large number of manuscript files, or there were many other Portal users uploading files simultaneously, it is possible that some of your files were not yet processed. You will be able to determine which files are still unprocessed by clicking on the conference title.

Viewing Results

To view the CrossCheck Similarity Reports for the processed files, you must log into the Portal and go to the “My Publications” page. Click on the title of your publication, and you will be brought to the Reports page. You will see the following columns on the page

- Date Processed (this is the date your file was uploaded and processed)
- File Name (the file name used for each manuscript file uploaded)
- Similarity % (how much of the uploaded manuscript matches previously published material)
- Results (if the similarity percentage is under 30%, the Results column text will say OK. If not, it will say “Review Report”)

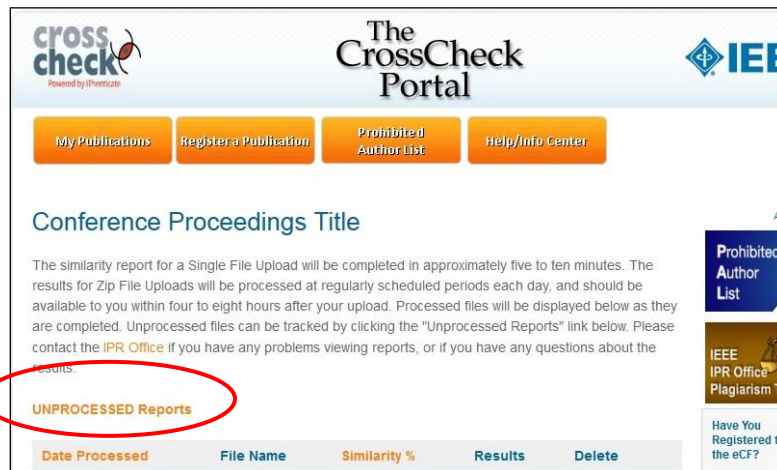
The screenshot displays the 'The CrossCheck Portal' interface. At the top, there are navigation buttons: 'My Publications', 'Register a Publication', 'Prohibited Author List', and 'Help/Info Center'. The IEEE logo is also present. Below the navigation bar, the page title is 'Conference Proceedings Title'. A paragraph explains the similarity report process: 'The similarity report for a Single File Upload will be completed in approximately five to ten minutes. The results for Zip File Uploads will be processed at regularly scheduled periods each day, and should be available to you within four to eight hours after your upload. Processed files will be displayed below as they are completed. Unprocessed files can be tracked by clicking the "Unprocessed Reports" link below. Please contact the IPR Office if you have any problems viewing reports, or if you have any questions about the results.'

Below this text, there is a section titled 'UNPROCESSED Reports' which contains a table with the following data:

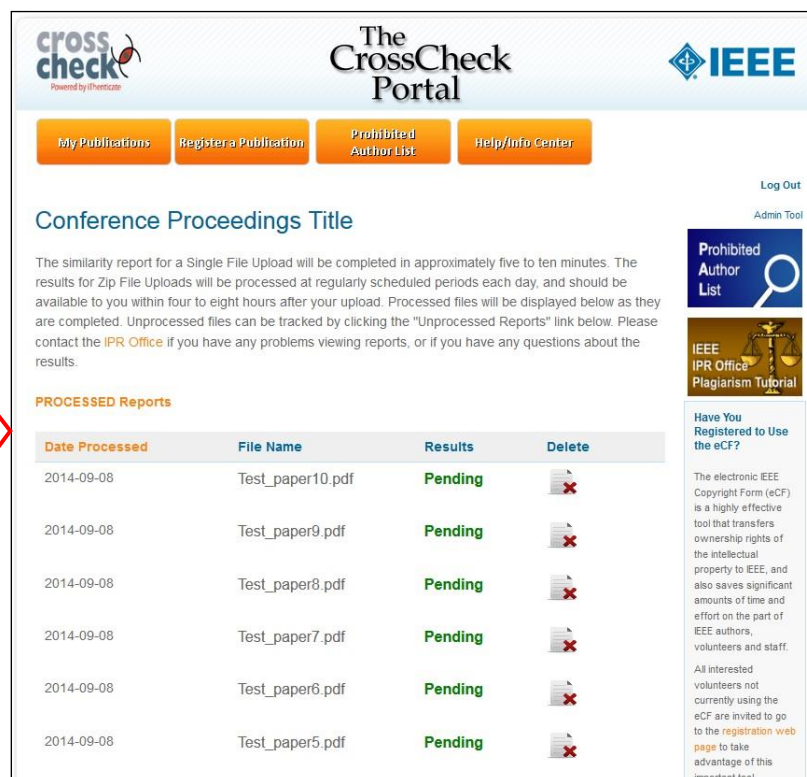
Date Processed	File Name	Similarity %	Results	Delete
2014-09-08	Test_paper2.pdf	45.0	Review Report	
2014-09-08	Test_paper4.pdf	45.0	Review Report	
2014-09-08	Test_paper5.pdf	28.0	OK	
2014-09-08	Test_paper9.pdf	28.0	OK	

On the right side of the interface, there are several links and a tutorial: 'Log Out', 'Admin Tool', 'Prohibited Author List' (with a magnifying glass icon), 'IEEE IPR Office Plagiarism Tutorial' (with a scales icon), and 'Have You Registered to Use the eCF?' (with a text box explaining the eCF form).

At the top of the table is a link to “Unprocessed Reports” which will allow you to check if any manuscript files are still being processed by CrossCheck. Clicking the link will bring you to the Unprocessed Results page. Files that are listed in the Unprocessed Reports view will show a “Pending” status in the Results Column. Clicking the line “Processed Reports” will bring you back to the Results Page.



The screenshot shows the top of the CrossCheck Portal. At the top, there are logos for 'cross check' (Powered by iThenticate), 'The CrossCheck Portal', and 'IEEE'. Below these are four orange buttons: 'My Publications', 'Register a Publication', 'Prohibited Author List', and 'Help/Info Center'. A section titled 'Conference Proceedings Title' contains a paragraph about similarity reports. Below this paragraph, the link 'UNPROCESSED Reports' is circled in red. At the bottom, a table header is visible with columns: 'Date Processed', 'File Name', 'Similarity %', 'Results', and 'Delete'.



The screenshot shows the 'PROCESSED Reports' page. It has the same header as the previous screenshot. Below the 'Conference Proceedings Title' section, the link 'PROCESSED Reports' is highlighted. Below this is a table with the following data:

Date Processed	File Name	Results	Delete
2014-09-08	Test_paper10.pdf	Pending	
2014-09-08	Test_paper9.pdf	Pending	
2014-09-08	Test_paper8.pdf	Pending	
2014-09-08	Test_paper7.pdf	Pending	
2014-09-08	Test_paper6.pdf	Pending	
2014-09-08	Test_paper5.pdf	Pending	

A red arrow points from the 'UNPROCESSED Reports' link in the previous screenshot to the 'PROCESSED Reports' section in this screenshot.

Any unprocessed files should be completed within another 4 to 8 hours. Please contact the IPR Office at crosscheckportal@ieee.org if any files remain unprocessed for over 24 hours.

Once the files have been processed, reports can be sorted by Date Processed or Similarity %. Clicking on the “Results” in the right column will launch a pop-up window **(be sure to deactivate any pop-up blockers on your web browser)** with a detailed Similarity Report from CrossCheck with highlighted text to show the portions of the submitted manuscript that are similar to other sources.

Interpreting the Results

You will be pleased to know that dedicated IEEE IPR Office staff are monitoring the Portal, and will review incoming results for any potential problems. Staff will identify the most problematic issues and will notify you if there is a problem that needs your attention. We encourage you to review the Alerts as well, and to contact Staff if you find anything that you think could be a problem.

Part 2. Reviewing and Interpreting Similarity Reports

Introduction

By now, you have begun using CrossCheck and have found manuscripts with a range of different similarity levels. Now what do you do?

The first thing to understand is that nearly every paper scanned by CrossCheck will detect SOME similarity to another source. This doesn't mean that every paper is suspect. There is only a concern if CrossCheck:

- Detects a substantial amount of text in the paper that has been duplicated from an original source, and
- The text from the original source is not cited in the paper

By following a few simple steps, you can quickly evaluate a large number of submissions and pinpoint any papers that may have problems.

Understanding Similarity Scores

It's important to keep in mind that the percentage level of each similarity report can contain several individual sources (sometimes as many as 20 or more). These individual sources each has its own similarity percentage that is combined into the full report's similarity percentage shown in the Folder View. For example, a paper with a similarity report of 20% may have 20 individual sources, each with only 1% of similar text, which can represent commonly used phrases.

There are three categories for similarity percentage ranges to keep in mind when reviewing a group of submitted manuscripts in CrossCheck:

< 10% Low Percentage = Not Likely to Be an Issue (Disregard) The similarity found in these papers is sporadic matching text or commonly used phrases. Single sources normally only yield 1-3% similarity. These reports may be disregarded.

10-50% Moderate Percentage = Possible Issue (Review Briefly) Papers that fall in this range may contain portions of copied text that are of some concern, but this depends on the percentage of similarity in the individual sources. Opening and briefly reviewing these reports can ensure that no individual source has more than 10% similarity.

> 50% High Percentage = Probable Issue (Review Carefully) At this level, the report percentage is automatically highlighted by CrossCheck in orange. These reports require a more careful review. There is likely to be a high percentage of similarity to one or more source.

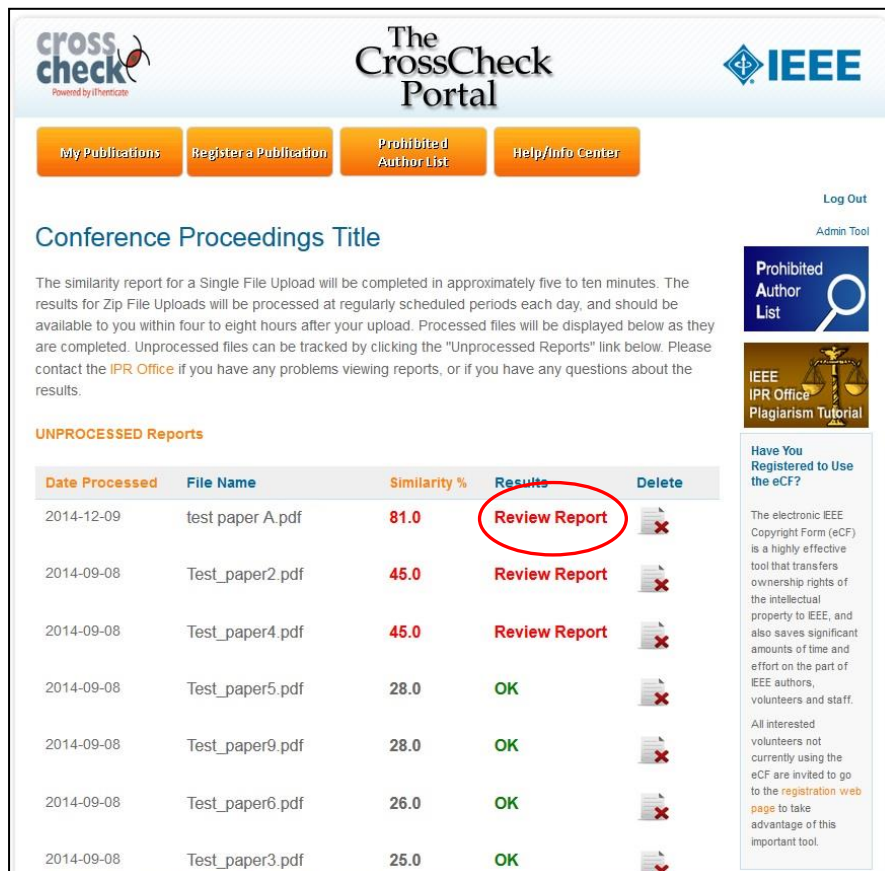
Factors to Keep in Mind when Reviewing Reports

False Alarms--A false alarm paper yields a similarity percentage higher than 30% but shows no sign of plagiarism in the report. The *overall* percentage is high but there are many different sources which all yield 5% or less. These papers need only a brief review.








Hidden Problems--Hidden problems are papers that look acceptable on the surface but show possible plagiarism upon review of the report. They generally have a low overall similarity percentage but yield a high percentage from a single source. For example, a paper with a 12% similarity level (which is nearly a negligible amount) may only have two individual sources. One source may have 1% of similar text, while the other source has 11% of similar text (which may include several copied paragraphs of text). These reports should be reviewed carefully.

Reviewing a Similarity Report

After you have clicked on your publication title, you will arrive on the Results page. Choose a report to open by clicking on the link to the right of the Similarity %. As an example, we have chosen a paper that had a substantial level of similarity (81%).



The screenshot displays the 'The CrossCheck Portal' interface. At the top, there are navigation buttons: 'My Publications', 'Register a Publication', 'Prohibited Author List', and 'Help/Info Center'. The main heading is 'Conference Proceedings Title'. Below this, a paragraph explains the similarity report process. A table titled 'UNPROCESSED Reports' lists several files. The first row, 'test paper A.pdf', has a similarity of 81.0 and a 'Review Report' link circled in red. The other rows show files with lower similarity percentages (45.0, 45.0, 28.0, 28.0, 26.0, 25.0) and 'OK' status. On the right side, there are links for 'Log Out', 'Admin Tool', 'Prohibited Author List', 'IEEE IPR Office Plagiarism Tutorial', and a section titled 'Have You Registered to Use the eCF?' with a brief description of the eCF tool.

Date Processed	File Name	Similarity %	Results	Delete
2014-12-09	test paper A.pdf	81.0	Review Report	
2014-09-08	Test_paper2.pdf	45.0	Review Report	
2014-09-08	Test_paper4.pdf	45.0	Review Report	
2014-09-08	Test_paper5.pdf	28.0	OK	
2014-09-08	Test_paper9.pdf	28.0	OK	
2014-09-08	Test_paper6.pdf	26.0	OK	
2014-09-08	Test_paper3.pdf	25.0	OK	

After clicking on the results link, a new page opens to show the full report (**be sure to deactivate any pop-up blockers on your web browser**). The two-panel report page shows a list of sources on the right side. The first source has a 23% similarity. This is a potential problem that should be checked more carefully.

The screenshot displays the iThenticate web interface. The top header shows the document title 'test paper A.pdf' by 'ANTHONY VENGRAITIS' and a similarity score of '81%'. The left panel shows the document content, which includes a title 'DATA ACCOUNTABILITY IN CLOUD USING RELIABLE LOG FILES FORWARDING' and an abstract. The right panel, titled 'Match Overview', lists ten matches. The first match is circled in red, indicating a 23% similarity from 'Internet' (633 words, crawled on 27-Aug-2013, vidhatha.com). The other matches show lower similarity percentages: 18%, 9%, 6%, 5%, 3%, 2%, 2%, 2%, and 2%.

Match Number	Source	Words	Crawled On	Similarity
1	Internet	633 words	27-Aug-2013	23%
2	Internet	493 words	28-Nov-2013	18%
3	Internet	261 words	09-Oct-2013	9%
4	Internet	173 words	27-Feb-2014	6%
5	Internet	151 words	18-Sep-2014	5%
6	CrossCheck	73 words	Sundareswaran, Smitha, Anna Squicciarini, and Dan Lin	3%
7	Internet	67 words	crawled on 27-Feb-2014	2%
8	Internet	63 words	crawled on 09-Oct-2014	2%
9	Internet	62 words	crawled on 24-Jul-2013	2%
10	Internet	61 words	crawled on 18-Jul-2013	2%

Clicking on the number “1” on the right panel will bring the first instance of similarity in the submitted text to the top of the left panel. A corresponding number “1” can be found on the matching text. The color of the source link (red) will match the color of the similar text in the submission. The bar at the top of the right panel will also show the number of matches for that source in the manuscript.

09-Dec-2014 03:23PM 2719 words • 77 matches • 22 sources

iThenticate test paper A.pdf BY ANTHONY VENGRATIS

Quotes Included Bibliography Included **81%** SIMILAR

Match Overview Match 1 of 29

Rank	Source	Words	Matched	Percentage
1	Internet 633 words crawled on 27-Aug-2013 vidhatha.com	633	145	23%
2	Internet 493 words crawled on 28-Nov-2013 www.ijcta.com	493	89	18%
3	Internet 261 words crawled on 09-Oct-2013 ijptjournal.org	261	24	9%
4	Internet 173 words crawled on 27-Feb-2014 www.ijcsmr.org	173	10	6%
5	Internet 151 words crawled on 18-Sep-2014 ljarcet.org	151	8	5%
6	CrossCheck 73 words Sundareswaran, Smitha, Anna Squicciarini, and Dan Lin "Ensuring Distributed Accountability for Data Sharing ..."	73	2	3%
7	Internet 67 words crawled on 27-Feb-2014 ijrcet.org	67	1	2%
8	Internet 63 words crawled on 09-Oct-2014 www.esignit.org	63	1	2%
9	Internet 62 words crawled on 24-Jul-2013 www.super-visions.com	62	1	2%
10	Internet 61 words crawled on 18-Jul-2013 www.iisce.org	61	1	2%

DATA ACCOUNTABILITY IN CLOUD USING RELIABLE LOG FILES FORWARDING

R.N.Heames II-M.E.(CSE),
MKCE, Karur - 639 113.
Email: mhheames@gmail.com

Dr.P.SUDHAKAR M.Tech., Ph.D.,
HOD / CSE.
MKCE, Karur - 639 113.

Internet vidhatha.com Full Source View

o the dynamic nature of the cloud. More specifically, log files should be tightly bounded with the corresponding data being controlled, and require minimal infrastructural support from any server. 2. Every access to the user's data should be correctly and automatically logged. This requires integrated techniques to authenticate the entity who accesses the data, verify, and record the actual operations on the data as well as the time that the data have been accessed. 3. L

INTRODUCTION

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. The data processed on clouds are often outsourced, leading to a number of issues related to accountability, including the handling of personally identifiable information. Such fears are becoming a significant barrier to the wide adoption of cloud services. It is essential to provide an effective mechanism for users to monitor the usage of their data in the cloud

service provider (CSP) to other entities in the cloud and these entities can also delegate the tasks to others, and so on. Second, entities are allowed to join and leave the cloud in a flexible manner. As a result, data handling in the cloud goes through a complex and dynamic hierarchical service chain which does not exist in conventional environments.

To overcome the above problems, a novel approach, namely Cloud Information Accountability (CIA) [01] framework was proposed, based on the notion of information accountability. Information account-ability focuses on keeping the data usage transparent and traceable. The proposed CIA framework provides

Internet vidhatha.com **A** Full Source View

o the dynamic nature of the cloud. More specifically, log files should be tightly bounded with the corresponding data being controlled, and require minimal infrastructural support from any server. 2. Every access to the user's data should be correctly and automatically logged. This requires integrated techniques to authenticate the entity who accesses the data, verify, and record the actual operations on the data as well as the time that the data have been accessed. 3. L

B

A pop-up window also will appear when clicking the sources on the right. The pop-up window shows (A) a link to the web site or publisher's digital library with the original content, and (B) a link to view the matching content side-by-side with the submitted manuscript.

09-Dec-2014 03:23PM 2719 words • 65 matches • 1 source

iThenticate® test paper A.pdf BY ANTHONY VENGARITIS

Quotes Included Bibliography Included 81% SIMILAR

Full Source Text

Internet
http://idhatha.com/Upload/JAW/IEEE12/BASEPAPER/JI
E1201%20-%20BasePaper.pdf 68%

Match 1 of 65

IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 4, JULY/AUGUST 2012 555 Ensuring Distributed Accountability for Data Sharing in the Cloud Smitha Sundareswaran, Anna C. Squicciarini, Member, IEEE, and Dan Lin Abstract—Cloud computing enables highly scalable services to be easily consumed over the Internet on an as-needed basis. A major feature of the cloud services is that users' data are usually processed remotely in unknown machines that users do not own or operate. While enjoying the convenience brought by this new emerging technology, users' fears of losing control of their own data (particularly, financial and health data) can become a significant barrier to the wide adoption of cloud services. To address this problem, in this paper, we propose a novel highly decentralized information accountability framework to keep track of the actual usage of the users' data in the cloud. In particular, we propose an object-centered approach that enables enclosing our logging mechanism together with users' data and policies. We leverage the JAR programmable capabilities to both create a dynamic and traveling object, and to ensure that any access to users' data will trigger authentication and automated logging local to the JARs. To strengthen user's control, we also provide distributed auditing mechanisms. We provide extensive experimental studies that demonstrate the efficiency and effectiveness of the proposed approaches. Index Terms—Cloud computing, accountability, data sharing. C 1 INTRODUCTION CLOUD computing presents a new way to supplement the current consumption and delivery model for IT services based on the Internet, by providing for dynamically scalable and often virtualized resources as a service over the Internet. To date, there are a number of notable commercial and individual cloud computing services, including Amazon, Google, Microsoft, Yahoo, and Salesforce [19]. Details of the services provided are abstracted from the users who no longer need to be experts of technology infrastructure. Moreover, users may not know the machines which actually process and host their data. While enjoying the convenience brought by this new technology, users also start worrying about losing control of their own data. The data processed on clouds are often outsourced, leading to a number of issues related to accountability, including the handling of personally identifiable information. Such fears are becoming a significant barrier to the wide adoption of cloud services [30]. To allay users' concerns, it is essential to provide an effective mechanism

storage device, the cloud takes away that step. The cloud removes the need for you to be in the same physical location as the hardware that stores your data. A major feature of the cloud services is that user data are usually processed remotely in unknown machines that users do not own or operate. Data handling in the cloud goes through a complex and dynamic hierarchical service chain which does not exist in conventional environments. This can be addressed by a novel approach, namely Cloud Information Accountability (CIA) framework. In this every access to the data are correctly and automatically logged. Log files are sent back to their data owners periodically to inform them of the current usage of their data. More importantly, files should be retrievable any time by their data owners when needed regardless the location where the files are stored. The end user is allowed to access the data as per their access privileges which they specifies while registering to access the data in the cloud and authentication is provided and accessed data is verified with the original data in the cloud server.

L INTRODUCTION

Cloud computing is the use of computing resources (hardware and software) that are delivered as a service over a network (typically the Internet). The name comes from the use of a cloud-shaped symbol as an abstraction for the complex infrastructure it contains in system diagrams. Cloud computing entrusts remote services with a user's data, software and computation. The data processed on clouds are often outsourced, leading to a number of issues related to accountability, including the handling of personally identifiable information. Such fears are becoming a significant barrier to the wide adoption of cloud services. It is essential to provide an effective mechanism for users to monitor the usage of their data in the cloud. Conventional access control approaches developed for closed domains such as databases and operating systems, or approaches using a centralized server in distributed environments, are not suitable, due to the following features characterizing cloud environments. First, data handling can be outsourced by the direct cloud service provider (CSP) to other entities in the cloud and these entities can also delegate the tasks to others, and so on. Second, entities are allowed to join and leave the cloud in a flexible manner. As a result, data handling in the cloud goes through a complex and dynamic hierarchical service chain which does not exist in conventional environments.

To overcome the above problems, a novel approach, namely Cloud Information Accountability (CIA) [01] framework was proposed, based on the notion of information accountability. Information account-ability focuses on keeping the data usage transparent and traceable. The proposed CIA framework provides end-to-end accountability in a highly distributed fashion. By means of the CIA [02], data owners can track not only whether or not the service-level agreements are being honoured, but also enforce access and usage control rules as needed. Associated with the accountability feature two distinct modes for auditing: push mode and pull mode.

The push mode refers to logs being periodically sent to the data owner or stakeholder while the pull mode refers to an alternative approach whereby the user (or another authorized authentication or storage system in place.

Beyond traditional access control in that a certain degree of usage control was provided for the protected data after these are delivered to the receiver [05]. [06].

PAGE: 2 OF 5

By scrolling to the end of the submission and reviewing the references, we see that the matching text was included as a reference. But based on the extent of content that was copied, it would still be inappropriately reused.

09-Dec-2014 03:23PM 2719 words • 65 matches • 1 source

iThenticate® test paper A.pdf BY ANTHONY VENGARITIS

Quotes Included Bibliography Included 81% SIMILAR

Full Source Text

Internet
http://idhatha.com/Upload/JAW/IEEE12/BASEPAPER/JI
E1201%20-%20BasePaper.pdf 68%

Match 1 of 65

IEEE TRANSACTIONS ON DEPENDABLE AND SECURE COMPUTING, VOL. 9, NO. 4, JULY/AUGUST 2012 555 Ensuring Distributed Accountability for Data Sharing in the Cloud Smitha Sundareswaran, Anna C. Squicciarini, Member, IEEE, and Dan Lin Abstract—Cloud computing enables highly scalable services to be easily consumed over the Internet on an as-needed basis. A major feature of the cloud services is that users' data are usually processed remotely in unknown machines that users do not own or operate. While enjoying the convenience brought by this new emerging technology, users' fears of losing control of their own data (particularly, financial and health data) can become a significant barrier to the wide adoption of cloud services. To address this problem, in this paper, we propose a novel highly decentralized information accountability framework to keep track of the actual usage of the users' data in the cloud. In particular, we propose an object-centered approach that enables enclosing our logging mechanism together with users' data and policies. We leverage the JAR programmable capabilities to both create a dynamic and traveling object, and to ensure that any access to users' data will trigger authentication and automated logging local to the JARs. To strengthen user's control, we also provide distributed auditing mechanisms. We provide extensive experimental studies that demonstrate the efficiency and effectiveness of the proposed approaches. Index Terms—Cloud computing, accountability, data sharing. C 1 INTRODUCTION CLOUD computing presents a new way to supplement the current consumption and delivery model for IT services based on the Internet, by providing for dynamically scalable and often virtualized resources as a service over the Internet. To date, there are a number of notable commercial and individual cloud computing services, including Amazon, Google, Microsoft, Yahoo, and Salesforce [19]. Details of the services provided are abstracted from the users who no longer need to be experts of technology infrastructure. Moreover, users may not know the machines which actually process and host their data. While enjoying the convenience brought by this new technology, users also start worrying about losing control of their own data. The data processed on clouds are often outsourced, leading to a number of issues related to accountability, including the handling of personally identifiable information. Such fears are becoming a significant barrier to the wide adoption of cloud services [30]. To allay users' concerns, it is essential to provide an effective mechanism

by a user, employ dual-phase authentication, where in a trusted identity provider issues certificates verifying the user's identity based on his username.

Once the authentication succeeds, the service provider (or the user) will be allowed to access the data enclosed in the JAR. Depending on the configuration settings defined at the time of creation, the JAR will provide usage control associated with logging, or will provide only logging functionality. As for the logging, each time there is an access to the data then the JAR will automatically generate a log record, encrypt it using the public key distributed by the data owner, and store it along with the data (step 6). The encryption of the log file prevents unauthorized changes to the file by attackers. The data owner could opt to reuse the same key pair for all JARs or create different key pairs for separate JARs. Using separate keys can enhance the security without introducing any overhead except in the initialization phase. In addition, some error correction information will be sent to the log handler to handle possible log file corruption. To ensure trustworthiness of the logs, each record is signed by the entity accessing the content. Further, individual records are hashed together to create a chain structure, able to quickly detect possible errors or missing records. The encrypted log files can later be decrypted and their integrity verified. They can be accessed by the data owner or other authorized stakeholders at any time for auditing purposes with the aid of the log harmoniser (step 9).

4. AUTOMATED LOGGING MECHANISM

4.1 The Logger Structure

The main responsibility of the outer JAR is to handle authentication of entities which want to access the data stored in the JAR file. In the context, the data owners may not know the CSPs that are going to handle the data. Hence authentication is performed according to the servers' functionality, rather than the server's

center terms as opposed to the usual code-centric security offered by Java, using Java Authentication and Authorization Services. Moreover, the outer JAR is also in charge of selecting the correct inner JAR according to the identity of the entity who requests the data.

Each inner JAR contains the encrypted data class files to facilitate retrieval of log files and display enclosed data in a usable format, and a log file for each encrypted item. It supports two options:

- Pure Log: Its main task is to record every access to the data. The log files are used for pure auditing purpose.
- Access Log: It has two functions: logging actions and enforcing access control. In case an access request is denied, the JAR will record the time when the request is made. If the access request is granted, the JAR will additionally record the access information along with the duration for which the access is allowed.

5. CONCLUSION

Innovative approaches for automatically logging any access to the data in the cloud together with an auditing mechanism and user access privilege. Data access can be controlled by implementing the user privilege. Moreover, one of the main features of the work is that it enables the data owner to audit even those copies of its data that were made without his knowledge. The end user can able to verify the accessed data from the cloud.

REFERENCES

[01] Anna C. Squicciarini, Smitha Sundareswaran, Ensuring Distributed Accountability for Data Sharing in the Cloud, IEEE Transactions On Dependable And Secure Computing, Vol. 9, No. 4, July/August 2012.

[02] M. Croso and G. Ruffo, "Reasoning About Accesses in a Distributed Environment, Third

PAGE: 4 OF 5

Interpreting Matching Percentages of Individual Sources

It may seem that any source of matching text should be a concern, but in fact many matching sources are likely to not be the result of plagiarism. For example:

< 1%-3% match—Occurs with small groups of similar words or a few short phrases. In general, there is little need to review these sources.

4-7% match—These matches can be similar single sentences or a small paragraph. One source at this level may not be an issue, but several sources at this percentage level could signify an overall problem with the submission.

8-15% match—A source in this percentage range usually involves a few matching paragraphs. Similarity at this level could indicate improperly reused material.

15-25% match—This level of similarity in a single source likely involves as much as one full page of matching material, depending on the size of the submission. It is important to check matches carefully against the source.

>25% match—This level of similarity from a single source should raise serious concerns about inappropriate reuse, and should be checked very carefully.

Factors to Keep in Mind when Reviewing Individual Sources

Is the similarity to the authors' own work?

This can often be the case. Authors build upon their own previously published work, and will often reuse portions of text. While this would not be considered plagiarism, it may still indicate a potential problem if the reuse of previously published content is not cited properly.

Is the similarity to work that has been properly cited in the submission?

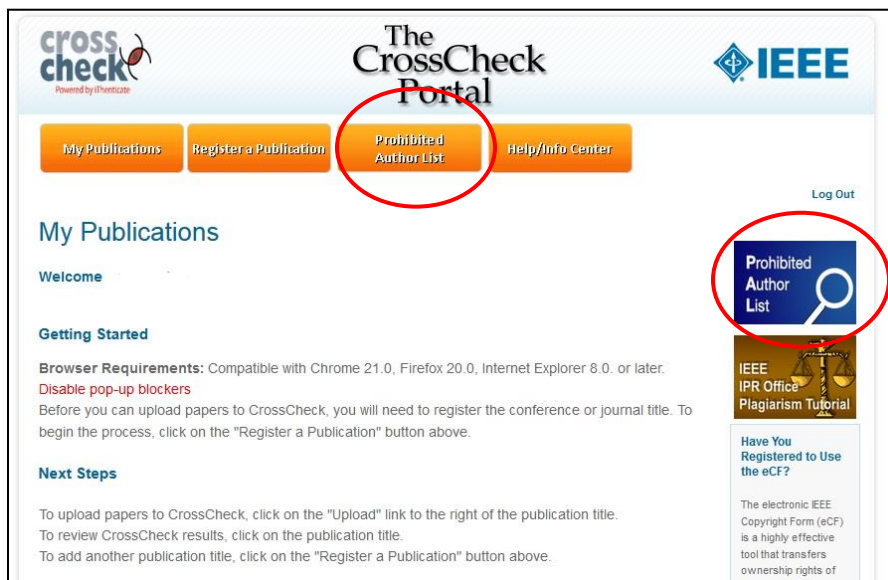
As shown in the example in Section 3, checking the submission's reference list can determine if the similar text was reused with an appropriate attribution to the source. It is also possible that the similarity between the two papers is because both authors (submitting author and source author) have used the same portion of text taken from another source.

Part 3. Overview of the IEEE Prohibited Authors List Database

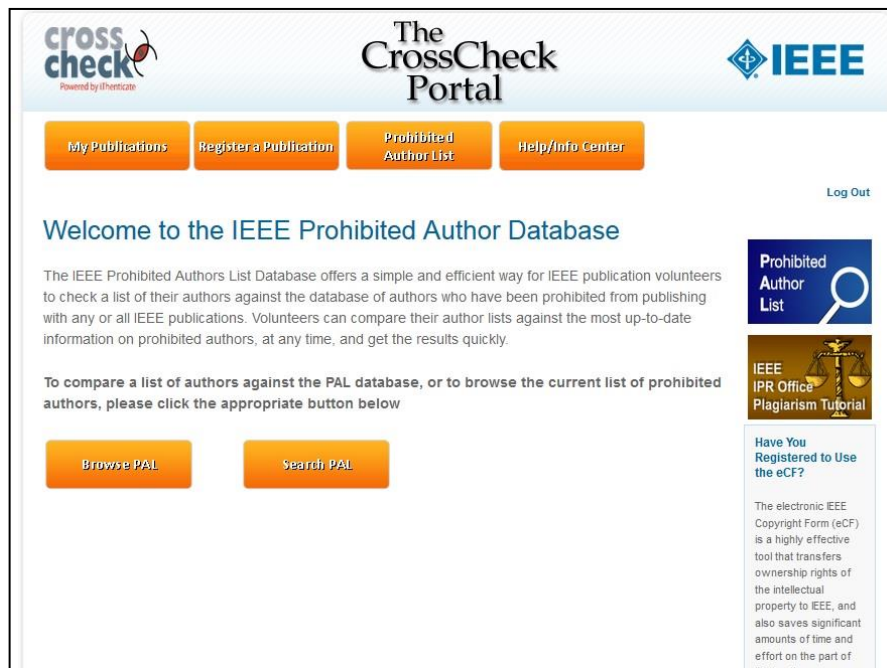
An important tool in ensuring the high quality of IEEE's publications is the Prohibited Authors List (PAL). This list contains the names of authors who have been banned from publishing in IEEE's journals and conferences because they were found to have violated IEEE's publishing conduct guidelines – usually because of significant plagiarism. To make this tool easier to use, the Intellectual Property Rights Office introduced the online database version of the PAL.

The PAL Database includes an automated tool that compares a spreadsheet of author names and email addresses against the database of prohibited authors, and presents the results on screen (or in a downloadable file). The Database also allows users to input an individual author's name or email address for quick comparison against PAL metadata, or to browse the names alphabetically.

Finding the PAL Database in the CrossCheck Portal



There are two links to the PAL Database tool from the main page of the CrossCheck Portal. Either the second tab at the top of the page, or the blue graphic on the right side of the page can be clicked to bring us to the PAL Database landing page.



From the landing page, users will have two options.

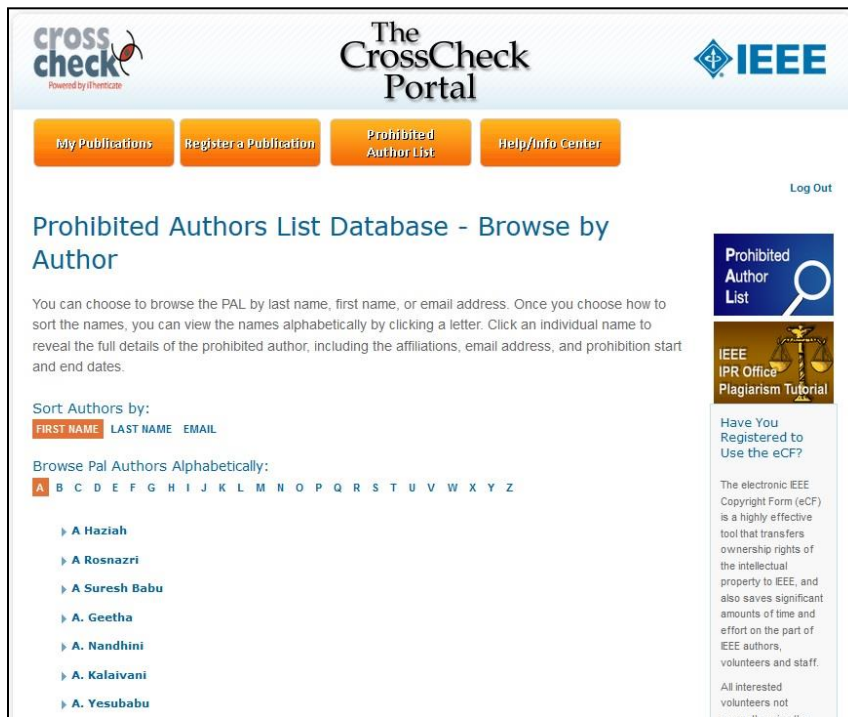


Browse PAL: Allows users to view all prohibited authors alphabetically, either by first name, last name, or email address.

Search PAL: Provides an automated tool to compare a spreadsheet of author names and email addresses against the database of prohibited authors. Results are presented on screen or in a downloadable file. Also allows users to input an individual author's name or email address for quick comparison against PAL metadata.

Browse PAL Page

From this page, users can click on the “Sort Authors by” choice of either First Name, Last Name, or Email Address. Once selected, the user can click on the desired letter of the alphabet to see all prohibited authors that are listed under that letter.






Search PAL

From this page, users can input the data of their author(s) and have the PAL Database Tool compare this data against the database of prohibited authors, and any matching authors will be displayed on a results page. Users have two options for searching. For a small number of authors (or just a single author), users may find the Single Name Input Tool to be the easiest option. For a large number of authors, users will likely want to use the spreadsheet upload feature.

Single Name Input Tool: Users can simply add the first name, last name, and email address of any author and then click “Search” to have the PAL Database compare the name instantly to all prohibited authors. The results will be displayed online, along with all relevant details of the prohibited author.

Spreadsheet Upload Tool: Users will need to first download the blank spreadsheet from the site. The link to the spreadsheet is highlighted in the directions on the page. Once the data has been added to the spreadsheet, the user can click on the Excel File Upload link to launch the upload tool. After uploading the spreadsheet, the user will be brought to a results page to see any matching author names.



[My Publications](#)[Register a Publication](#)[Prohibited Author List](#)[Help/Info Center](#)

[Log Out](#)
[Admin Tool](#)

Prohibited Authors List Database--Search Tool

Getting started: There are two ways to use the PAL Database Search Tool. You can either check an individual author by using the Single Name Input Tool, or you can check a larger collection of authors by using the Spreadsheet Upload Tool. Both Tools compare your author details against the PAL database, and will show matching names (if any) on a Results page.

How to use the Single Name Input Tool

Input author information in the fields below. You must fill in at least one of the field in order to search the database. After entering the name, please click the Enter button.

Please complete at-least one fields

First Name:

Last Name:



Email:

[SEARCH](#)

How to use the Spreadsheet Upload Tool

1. To begin, please download the [PAL Spreadsheet\(Excel\)](#).
2. Next, input the following information for each author into the appropriate columns on the spreadsheet.
Author First Name Author Last Name Author Email Address
3. Once the spreadsheet is completed, upload the spreadsheet (only once) using the utility below:

[Excel File Upload](#)



Have You Registered to Use the eCF?

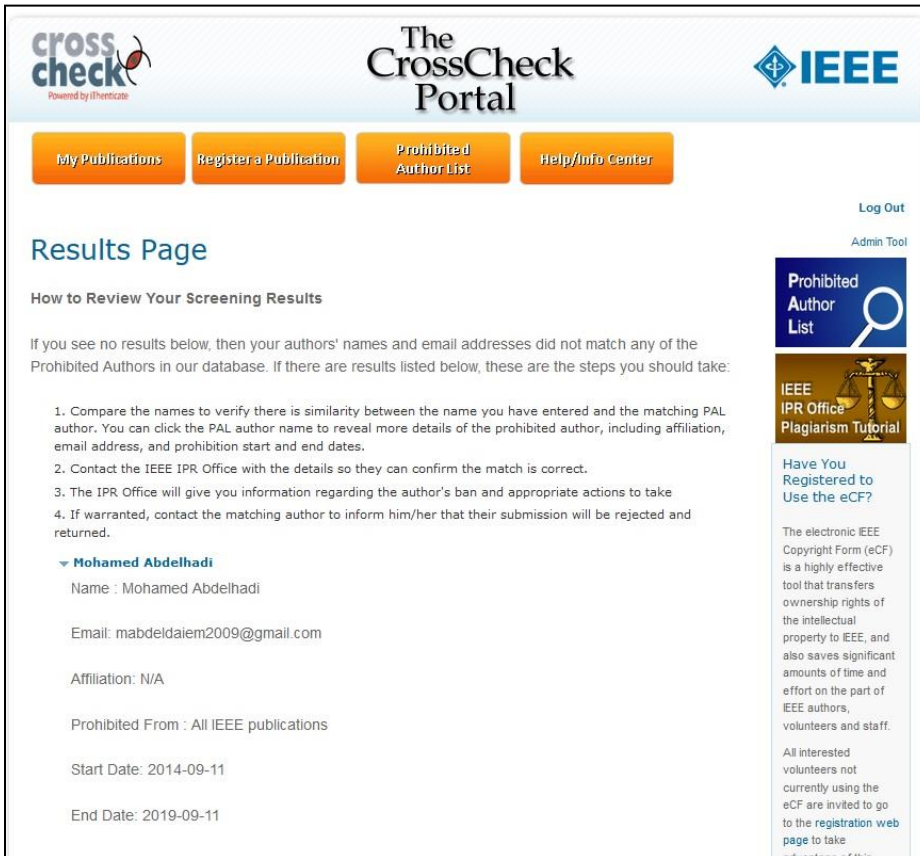
The electronic IEEE Copyright Form (eCF) is a highly effective tool that transfers ownership rights of the intellectual property to IEEE, and also saves significant amounts of time and effort on the part of IEEE authors, volunteers and staff.

All interested volunteers not currently using the eCF are invited to go to the [registration web page](#) to take advantage of this important tool.

[Support](#) | [Contact IEEE](#) | [IEEE Xplore Resources](#) | [Nondiscrimination Policy](#)

Results Page

Once users have submitted their author data to the PAL Database for comparison, they will be brought to a results page. From here, users can see how closely their authors matched any prohibited authors.



The screenshot shows the 'The CrossCheck Portal' interface. At the top, there are logos for 'cross check' (Powered by iThenticate), 'The CrossCheck Portal', and 'IEEE'. Below these are four orange buttons: 'My Publications', 'Register a Publication', 'Prohibited Author List', and 'Help/Info Center'. On the right side, there are links for 'Log Out' and 'Admin Tool'. The main heading is 'Results Page'. Below it, a section titled 'How to Review Your Screening Results' provides instructions on how to interpret the results. A specific result is shown for 'Mohamed Abdelhadi', including his name, email, affiliation, and the dates of prohibition. On the right sidebar, there are links for 'Prohibited Author List', 'IEEE IPR Office Plagiarism Tutorial', and a section titled 'Have You Registered to Use the eCF?' which explains the electronic IEEE Copyright Form (eCF).

cross check
Powered by iThenticate

The CrossCheck Portal

IEEE

My Publications Register a Publication Prohibited Author List Help/Info Center

Log Out
Admin Tool

Results Page

How to Review Your Screening Results

If you see no results below, then your authors' names and email addresses did not match any of the Prohibited Authors in our database. If there are results listed below, these are the steps you should take:

1. Compare the names to verify there is similarity between the name you have entered and the matching PAL author. You can click the PAL author name to reveal more details of the prohibited author, including affiliation, email address, and prohibition start and end dates.
2. Contact the IEEE IPR Office with the details so they can confirm the match is correct.
3. The IPR Office will give you information regarding the author's ban and appropriate actions to take
4. If warranted, contact the matching author to inform him/her that their submission will be rejected and returned.

▼ **Mohamed Abdelhadi**

Name : Mohamed Abdelhadi

Email: mabdeldaiem2009@gmail.com

Affiliation: N/A

Prohibited From : All IEEE publications

Start Date: 2014-09-11

End Date: 2019-09-11

Prohibited Author List

IEEE IPR Office Plagiarism Tutorial

Have You Registered to Use the eCF?

The electronic IEEE Copyright Form (eCF) is a highly effective tool that transfers ownership rights of the intellectual property to IEEE, and also saves significant amounts of time and effort on the part of IEEE authors, volunteers and staff.

All interested volunteers not currently using the eCF are invited to go to the registration web page to take advantage of this

It is important that publication volunteers **contact the IPR Office if there are any strong matches** to the PAL Database. IPR Office staff can review the records of the prohibited author against the data users have to confirm any match **before any decision is reached** on what actions to take.